Multi-step quantum algorithm for solving the 3-bit exact cover problem

Hefeng Wang*
Department of Applied Physics, Xi'an Jiaotong University, Xi'an 710049, China
Key Laboratory of Quantum Information and Quantum Optoelectronic Devices, Xi'an 710049, Shaanxi Province, China

We present a multi-step quantum algorithm for solving the 3-bit exact cover problem, which is one of the NP-complete problems. Unlike the brute force methods have been tried before, in this algorithm, we showed that by applying the clauses of the Boolean formula sequentially and introducing non-unitary operations, the state that satisfies all of the clauses can be projected out from an equal superposition of all computational basis states step by step, and the search space is reduced exponentially. The runtime of the algorithm is proportional to the number of clauses, therefore scales polynomial to the size of the problem. Our results indicate that quantum computers may be able to outperform classical computers in solving NP-complete problems.

PACS numbers: 03.67.Ac

I. INTRODUCTION

The mechanism of nature selection has produced the whole of Life on earth in a surprisingly short time of about three and half billion years. A computational question inspired by this phenomenon is [1] "what algorithm could possibly achieve all this in such a short time?" Can we develop algorithms using this mechanism? The 3-bit exact cover problem (EC3) is a hard problem in computer science and mathematics. In this problem, one has to find out if there exists an assignment(s) of an n-bit string that satisfies a Boolean formula of clauses. The EC3 problem shares similar property as the evolution of life: lives/assignments have to fit to the changing environments/clauses to survive. Here, we propose a multi-step quantum algorithm for solving this problem.

Quantum computing offers speedup in solving a number of problems [2–6]: factorizing large integers, searching unsorted databases, and simulating quantum systems, etc. The question of whether there are polynomial algorithms for NP-complete (NPC) problems is an unsolved problem in mathematics [7, 8]. The EC3 problem is a restricted version of the 3-bit satisfiability problem [9] and is one of the NPC problems. A quantum adiabatic algorithm was proposed for solving the EC3 problem on a quantum computer [9, 10], and it was found later that it cannot solve the EC3 problem efficiently [11–15]. The question of whether NPC problems can be solved in polynomial time on a quantum computer is an open question.

In most of the methods that have been tried, the EC3 problem is turned to a search problem directly. Classically, the cost for searching an item in a space of N items scales as $O(N)$. Grover's algorithm provides quadratic speedup over classical algorithms for the search problem on a quantum computer. While the cost can be reduced with the help of some tools. Let's see an example: there are 80 balls, all of them have equal weights except one that is lighter than the others. How to find out the lighter ball? If we randomly pick up a ball and compare its weight with the others, this will take about 40 trials on average. If we have a balance, then how many times do we have to use the balance to find out the lighter ball? According to information theory, the number of times the balance has to be used is $\log 80/\log 3 \approx 4$. The procedure is as follows: divide all the 80 balls into 3 groups, each group has 27, 27 and 26 balls, respectively. Pick up the two groups that both have 27 balls, and use the balance to determine if they have equal weights. If the answer is positive, pick the group with 26 balls and divide it into 3 groups again: $9, 9, 8$; otherwise, take the group that is lighter and divide it into three new groups, $9, 9, 9$. One can continue this process until the lighter ball is found.

From the above example, we can see that the search space is reduced exponentially by using the balance, therefore the cost of searching the target ball is reduced exponentially. In the algorithm we proposed in this work, by constructing a tool that has similar property as the balance and applying the clauses of the Boolean formula sequentially, the search space of the EC3 problem is reduced exponentially. The runtime of the algorithm is proportional to the number of clauses, therefore scales polynomial to the size of the problem.

II. THE ALGORITHM

The EC3 problem on a quantum computer can be formulated as follows: the 3-bit instance of satisfiability is a Boolean formula with M clauses

$$C_1 \wedge C_2 \wedge \cdots \wedge C_M, \tag{1}$$

where each clause C_l is true or false depending on the values of a subset of the n bits, and each clause contains three bits. The clause is true if and only if one of the three bits is 1 and the other two are 0. The task is to determine whether one (or more) of the 2^n assignments satisfies all of the clauses, that is, makes formula (1) true, and find the assignment(s) if it exists. Let i_C, j_C and k_C be the 3 bits associated with clause C, for each clause C,

* Correspondence to wanghf@mail.xjtu.edu.cn

we define a function

$$h_C(z_{i_C}, z_{j_C}, z_{k_C}) = \begin{cases} 0, \text{ if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ satisfies clause } C \\ 1, \text{ if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ violates clause } C. \end{cases} \tag{2}$$

The Hamiltonian for clause C is defined as

$$H_C|z_1 z_2 \cdots z_n\rangle = h_C\left(z_{i_C}, z_{j_C}, z_{k_C}\right)|z_1 z_2 \cdots z_n\rangle, \tag{3}$$

where $|z_j\rangle$ is the j-th bit and has value 0 or 1. If the ground state energy of the Hamiltonian H_C is zero, the ground state is a superposition of $|z_1 z_2 \cdots z_n\rangle$, where each bit string $z_1 z_2 \cdots z_n$ satisfies clause C. The dimension of computational basis states (CBS) $|z_1 z_2 \cdots z_n\rangle$ is $N = 2^n$. A solution to the EC3 problem is a state which is a superposition of CBS that satisfies all of the clauses, the eigenvalue of the state is zero for every Hamiltonian H_C for all of the clauses.

In this algorithm, we prepare an equal superposition of all CBS of n bits as initial state of the problem, and the clauses are applied in M steps sequentially. In each step, the state that satisfies the corresponding clause is projected out from the previous state. This procedure is based on resonance phenomenon. The eigenstates of the Hamiltonian H_C for clause C have eigenenergies of either 0 or 1, the energy of the ground state of H_C is 0 if it is an equal superposition of basis states that satisfy the clause C. For a probe qubit coupled to a system, the probe qubit exhibits dynamical response when it resonates with a transition in the system. The system can be guided to evolve to its ground state by inducing resonance between the probe qubit and a transition in the system [16]. Based on this idea, we can obtain the ground state of H_C with eigenvalue zero. A detailed procedure of the algorithm is as follows.

We construct a quantum register R of $(n+1)$ qubits, which contains one ancilla qubit and an n-qubit quantum register that represents the EC3 problem of dimension N. A probe qubit is coupled to R and the Hamiltonian of the entire $(n+2)$-qubit system is

$$H = -\frac{1}{2}\omega\sigma_z \otimes I_2^{\otimes(n+1)} + I_2 \otimes H_R + c\sigma_x \otimes \sigma_x \otimes I_N, \tag{4}$$

where I_2 and I_N are two- and N-dimensional identity operators, respectively, σ_x and σ_z are the Pauli matrices. The first term in the above equation is the Hamiltonian of the probe qubit, the second term is the Hamiltonian of the register R, and the third term describes the interaction between the probe qubit and R. Here, ω is the frequency of the probe qubit ($\hbar = 1$), and c is the coupling strength between the probe qubit and R, and $c \ll \omega$. The Hamiltonian of R is in the form

$$H_R = -1 \times |0\rangle\langle 0| \otimes I_N + |1\rangle\langle 1| \otimes H_C. \tag{5}$$

We set the frequency of the probe qubit as $\omega = 1$, and let $|\varphi_0\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle$ where $|j\rangle$ are the CBS of the n qubits. The procedure of the algorithm is as follows:

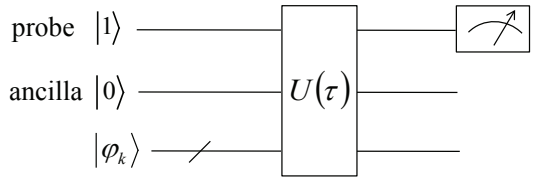

FIG. 1. Quantum circuit for solving the EC3 problem. The first line represents a probe qubit. $U(\tau)$ is a time evolution operator driven by a Hamiltonian in Eq. (4). The last n qubits represent the EC3 problem.

For $k = 1$:

(i) Prepare the probe qubit in its excited state $|1\rangle$ and the register R in state $|0\rangle|\varphi_{k-1}\rangle$, which is the eigenstate of H_R with eigenvalue -1.

(ii) Construct Hamiltonian H_{C_k} for clause C_k, and Hamiltonian H of the algorithm as shown in Eq. (4). Then implement time evolution operator $U(\tau) = \exp(-iH\tau)$ on the $(n+2)$-qubit system.

(iii) Read out the state of the probe qubit by performing a measurement on the probe qubit in its computational basis.

(iv) Repeat steps (i) – (iii) until a decay of the probe qubit is observed, and run a purification procedure as described below.

(v) Take the state of the last n qubits obtained from step (iv) as input state of the problem $|\varphi_k\rangle$. Set $k = k+1$, repeat steps (i)-(iv), until run over all of the M clauses.

The state $|\varphi_M\rangle$ of the last n qubits encodes the solution to the EC3 problem, that is, all assignments of the n bits that satisfy all of the M clauses. The quantum circuit for the $(k+1)$-th round of the algorithm is shown in Fig. 1.

In each round of the algorithm, the state in step (iv) of the algorithm can be purified to make it closer to the solution state of the round of the algorithm, that is, the eigenstate of the Hamiltonian H_C with eigenvalue 0, by performing partial measurements on the probe qubit [17]. This can be run on the circuit in Fig. 1. In step (iv) of the k-th round of the algorithm, when the measurement result on the probe qubit is in state $|0\rangle$, the state $|\varphi'_k\rangle$ of the last n qubits is set as the input state of the problem, and the clause Hamiltonian is unchanged. The entire $(n+2)$-qubit system is set in an initial state of $|1\rangle|0\rangle|\varphi'_k\rangle$, and evolve with Hamiltonian H for time $t_0 = \frac{\pi}{2c}$, then read out the state of the probe qubit by performing a measurement on the probe qubit. Repeat these steps until a decay of the probe qubit to its ground state is observed. This procedure can be repeated to improve the amplitude of the solution state of the round of the algorithm, while compress the amplitude of non-solution state of the algorithm. In each round of the algorithm, the purification procedure can be repeated for a number of times until a total number of M times of the measurements on the probe qubit are in its ground state $|0\rangle$.

III. EFFICIENCY OF THE ALGORITHM

We now analyze the efficiency of the algorithm. In the first round of the algorithm, the eigenstate $|\varphi_1\rangle$ obtained from the algorithm is the ground state of the Hamiltonian H_{C_1} with eigenvalue 0, which is an equal superposition of all CBS that satisfy clause C_1. The probability for obtaining the state $|\varphi_1\rangle$ is $p_1 = N_1/N = 3/8$, where N_1 is the number of CBS that satisfy clause C_1. In this round of the algorithm, the state space of the problem is reduced to $N_1 = p_1 \times N$.

In the second round of the algorithm, we set the state $|\varphi_1\rangle$ as input state of the problem, construct Hamiltonian H_{C_2} for clause C_2, and run the algorithm. The eigenstate $|\varphi_2\rangle$ of the Hamiltonian H_{C_2} with eigenvalue 0 is projected out from the state $|\varphi_1\rangle$ that satisfies clause C_1, therefore $|\varphi_2\rangle$ is an equal superposition of basis states that satisfy clauses $C_1 \wedge C_2$. The probability for obtaining state $|\varphi_2\rangle$ is $p_2 = N_2/N_1$ where N_2 is the number of CBS that satisfy clauses $C_1 \wedge C_2$. It depends on clause C_2, and can be one of the three values of $\{3/8, 5/12, 1/2\}$, which corresponds to the cases where clause C_2 has zero, one, or two bits same as clause C_1. In the second round, the state space of the problem is reduced to $N_2 = p_2 \times N_1 = p_2 p_1 \times N$.

In the third round of the algorithm, the state $|\varphi_2\rangle$ is set as input state of the problem, the Hamiltonian H_{C_3} is constructed for clause C_3. The eigenstate $|\varphi_3\rangle$ of the Hamiltonian H_{C_3} with eigenvalue 0 can be projected out from the state $|\varphi_2\rangle$. Since the state $|\varphi_2\rangle$ satisfies clauses $C_1 \wedge C_2$, the state $|\varphi_3\rangle$ is an equal superposition of basis states that satisfy clauses $C_1 \wedge C_2 \wedge C_3$. The probability $p_3 = N_3/N_2$ where N_3 is the number of CBS that satisfy clauses $C_1 \wedge C_2 \wedge C_3$. In the following we discuss possible values of p_3.

We define a function $S(C_k)$, which gives the number of bits in clause C_k that are same as that of in clause set $\{C_1, C_2, \cdots, C_{k-1}\}$ and $k \geqslant 3$. The function $S(C_k)$ can be $0, 1, 2$, or 3. We now discuss the possible values of $p_k = N_k/N_{k-1}$ for obtaining the state $|\varphi_k\rangle$ from state $|\varphi_{k-1}\rangle$ when $S(C_k)$ takes different values. It is obvious that $p_k = 3/8$ when $S(C_k) = 0$. For $S(C_k) = 1$, the smallest value that p_k can be is $p_k = 1/4$. In the case of $S(C_k) = 2$, the smallest value for p_k is 0, while the next smallest value of $p_k \geqslant 1/18$. For $S(C_k) = 3$, the smallest value of $p_k = 0$, and the next smallest value of $p_k \geqslant 1/27$. These estimations consider the maximal dimension of the state space that the bits in clause C_k associated with the clauses in the clause set $\{C_1, C_2, \cdots, C_{k-1}\}$.

From the above analysis, we can see that the smallest possible value of p_k is 0, while the next smallest value of p_k is finite. This means we can conclude whether the probability p_k for obtaining the state $|\varphi_k\rangle$ is zero or not in finite number of trials in each round of the algorithm.

In the following, we discuss the evolution time required for obtaining the eigenstate of a clause Hamiltonian with eigenvalue 0 in each round of the algorithm. We take the k-th round of the algorithm for obtaining state $|\varphi_k\rangle$ for instance.

In the k-th round, the input state of the problem is $|\varphi_{k-1}\rangle$, in basis of $\{|\Psi_0\rangle = |1\rangle|0\rangle|\varphi_{k-1}\rangle$, $|\Psi_1\rangle = |0\rangle|1\rangle|\varphi_k^{\text{sol}}\rangle$, $|\Psi_2\rangle = |0\rangle|1\rangle|\varphi_k^{\text{non-sol}}\rangle\}$, where states $|\varphi_k^{\text{sol}}\rangle = \frac{1}{\sqrt{N_k}} \sum_{r1=1}^{N_k} |j_{r1}\rangle$ and $|\varphi_k^{\text{non-sol}}\rangle = \frac{1}{\sqrt{N_{k-1}-N_k}} \sum_{r2=N_k+1}^{N_{k-1}} |j_{r2}\rangle$ are the eigenstates of H_{C_k} with eigenvalues 0 and 1, respectively, $|j_{r1}\rangle$ are the CBS that satisfy clauses $C_1 \wedge C_2 \wedge \cdots \wedge C_{k-1} \wedge C_k$, and $|j_{r2}\rangle$ are the CBS that satisfy clauses $C_1 \wedge C_2 \wedge \cdots \wedge C_{k-1}$ but do not satisfy clause C_k, the Hamiltonian H of the algorithm in Eq. (4) can be written as

$$H = \begin{pmatrix} -\frac{1}{2} & c\sqrt{p_k} & c\sqrt{1-p_k} \\ c\sqrt{p_k} & -\frac{1}{2} & 0 \\ c\sqrt{1-p_k} & 0 & \frac{1}{2} \end{pmatrix}, \tag{6}$$

where $p_k = N_k/N_{k-1}$. Let $|\Psi(t)\rangle = c_0(t)|\Psi_0\rangle + c_1(t)|\Psi_1\rangle + c_2(t)|\Psi_2\rangle$, the Schrödinger equation with the above Hamiltonian can be solved exactly and

$$c_1(t) = 2c\sqrt{p_k} \sum_x \frac{e^{-ixt} - 2xe^{-ixt}}{-12x^2 - 4x + 4c^2 + 1}, \tag{7}$$

where x are eigenvalues of the Hamiltonian matrix in Eq. (6).

When a decay of the probe qubit occurred, the state $|\Psi_0\rangle$ can be evolved to state $|\Psi_1\rangle$ with probability close to one at time $t = \frac{\pi}{2} \frac{1}{c\sqrt{p_k}}$, as long as p_k is finite. As we have discussed above, p_k is finite when $p_k \neq 0$. In Fig. 2, by setting $c = 0.02$ and $p_k = 1/27$, we show the variation of $|c_1(t)|^2$ and $|c_2(t)|^2$ with respect to evolution time t. The variation of $|c_2(t)|^2$ with respect to evolution time t is shown in Fig. 3. We can see that $|c_2(t)|$ is very small and in most of the evolution time $|c_1(t)|^2 \gg |c_2(t)|^2$. By running the algorithm for different evolution time to obtain the decay dynamics of the probe qubit [18], one can locate the optimal evolution time t in which the decay probability of the probe qubit reaches its maximal value and $|c_1(t)|$ is close to one. Consider the degeneracy of the eigenstates of the clause Hamiltonian with eigenvalues of 0 and 1, the probabilities of the system being in state $|\Psi_1\rangle$ and $|\Psi_2\rangle$ are $p_k|c_1(t)|^2$ and $(1-p_k)|c_2(t)|^2$, respectively. By running the purification procedure, the amplitude of the state $|\Psi_1\rangle$ can be greatly improved while the amplitude of the state $|\Psi_2\rangle$ can be compressed to be very small and close to zero in polynomial number of trials. This is analyzed in detail in the next section.

In the case of $p_k = 0$, the Hamiltonian H in basis of $\{|\Psi_0\rangle = |1\rangle|0\rangle|\varphi_{k-1}\rangle, |0\rangle|1\rangle \frac{1}{\sqrt{N_{k-1}}} \sum_{j=0}^{N_{k-1}-1} |j\rangle\}$ can be written as $H = \begin{pmatrix} -\frac{1}{2} & c \\ c & \frac{1}{2} \end{pmatrix}$. With the initial state being set as $|\Psi_0\rangle$, the decay probability of the probe qubit is $\frac{4c^2 \sin^2 \sqrt{1/4+c^2}t}{1+4c^2}$. It is very small for $c \ll 1$ and oscillates between 0 and $4c^2/(1+4c^2)$. The dynamics of the probe qubit in this case can be well distinguished from that of the probe qubit in the resonance case [18].

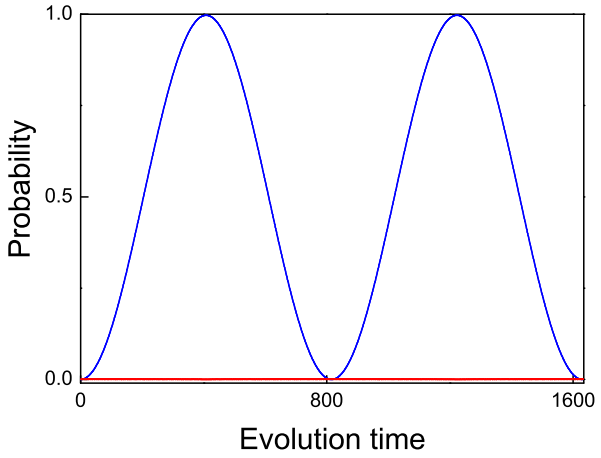

FIG. 2. (Color online) The variation of $|c_1(t)|^2$ and $|c_2(t)|^2$ vs. evolution time t in the k-th round of the algorithm, as $p_k = 1/27$ and $c = 0.02$. The blue curve shows the results for $|c_1(t)|^2$, while the red dot curve shows the results for $|c_2(t)|^2$.

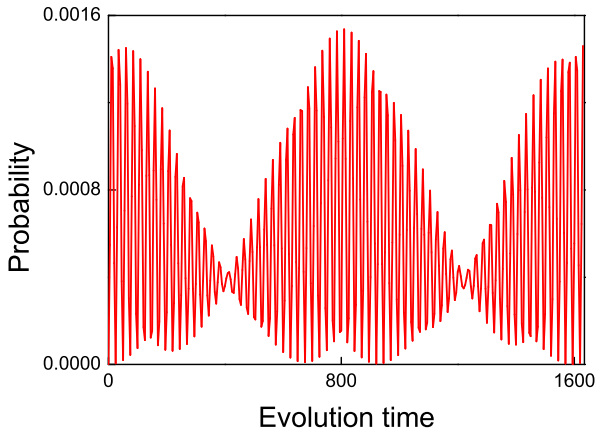

FIG. 3. (Color online) The variation of $|c_2(t)|^2$ vs. evolution time t in the k-th round of the algorithm, as $p_k = 1/27$ and $c = 0.02$.

In the algorithm, the total number of trials for executing the algorithm is proportional to the number of clauses M as $\propto \sum_{k=1,p_k\neq 0}^{M} \frac{1}{p_k}$. And since p_k is finite when $p_k \neq 0$, the amplitudes of the eigenstates that contain the solution to the problem can be amplified to close to unity in finite time by setting c to be small but finite. The maximum number of clauses for an n-bit string is $\binom{n}{3}$, in each round of the algorithm, the evolution time of the algorithm is finite when $p_k \neq 0$, and the case when $p_k = 0$ can be determined in finite number of trials. Therefore the runtime of the algorithm scales polynomial with the number of bits of the EC3 problem.

The time evolution operator $U(\tau) = \exp(-iH\tau)$ in the algorithm can be implemented efficiently through the Trotter formula [19] on a quantum computer.

The cost of the algorithm will be different if we apply the clauses in different order. We use an 8-bit EC3 problem as an example. The 3-bit sets of the 6 clauses $C_1, C_2, \cdots, C_6$ are applied in the order of $\{1,2,8\}$, $\{2,3,6\}$, $\{2,3,7\}$, $\{2,4,5\}$, $\{2,5,6\}$, and $\{3,5,8\}$. In this case, the corresponding probabilities of $p_1, p_2, \cdots, p_6$ are $\{3/8, 5/12, 1/2, 9/20, 5/9, 1/5\}$, respectively. The solution to the EC3 problem is $|00010111\rangle$. If we set the order of the 6 clauses as $\{2,3,6\}$, $\{2,3,7\}$, $\{2,5,6\}$, $\{2,4,5\}$, $\{3,5,8\}$, and $\{1,2,8\}$, the corresponding probabilities of $p_1, p_2, \cdots, p_6$ are $\{3/8, 1/2, 1/2, 1/2, 1/3, 1/4\}$. The cost of the algorithm is less in the second case.

IV. ERROR ANALYSIS

Suppose in the k-th round of the algorithm, the probability of the system being in state $|\Psi_2\rangle$ is ε, and in state $|\Psi_1\rangle$ is $1-\varepsilon$, then the success probability of the algorithm is $P_{\text{succ}} = (1-\varepsilon)^M \approx 1 - M\varepsilon + O(\varepsilon^2)$. This shows that the success probability of the algorithm can be very small when M is large. Fortunately, by running the purification procedure in each round of the algorithm, the state of the system can be purified to be very close to the solution state of the round of the algorithm, the error ε can be compressed to be very small such that the algorithm can still have high success probability. We now analyze the effect of the purification procedure in detail.

We define a measurement as "successful measurement" only if the measurement result on the probe qubit is in its ground state $|0\rangle$. In step (iv) of the k-th round of the algorithm, after a successful measurement on the probe qubit at evolution time $t = \frac{\pi}{2}\frac{1}{c\sqrt{p_k}}$, the entire system is collapsed to state $c_1'|\Psi_1\rangle + c_2'|\Psi_2\rangle$, where $|c_1'|^2 + |c_2'|^2 = 1$. We take the state of the last n qubits of the system as input state of the problem and run the purification procedure, the probability of the system being evolved to state $|\Psi_1\rangle$, which is the solution state of the round of the algorithm, can be further improved.

From Fig. 2 and Fig. 3, we can see that $|c_1'| \gg |c_2'|$ and $|c_1'|$ is close to one. Therefore in the purification procedure, we perform a measurement on the probe qubit after the system being evolved for time $t_0 = \frac{\pi}{2c}$. This guarantees that both the decay probability of the probe qubit and the probability of the system being evolved to the solution state of the round of the algorithm is close to one. If the measurement result on the probe qubit is in state $|1\rangle$, the state of the register R remain unchanged. When a successful measurement is performed, the operation acts on the register R is $V(t_0) = \langle 0|U(t_0)|0\rangle$, this operator in general is a non-unitary operator. In step (iv) of the algorithm, we can repeat the purification procedure until M successful measurements on the probe qubit are achieved, then the register R is evolved to state $[V(t_0)]^M|0\rangle|\varphi_k\rangle$. In basis of $\{|\Psi_1\rangle, |\Psi_2\rangle\}$, $V(t_0)$ is a two dimensional matrix whose eigenvalues λ_1 and λ_2 are discrete and non-degenerate and $|\lambda_1| > |\lambda_2|$. In this process, when M is large, the state of the register R converges to the eigenstate of $V(t_0)$ with corresponding eigenvalue λ_1 [17].

We now estimate the effect of the operator $V(t_0)$ acting on the register R. In step (iv) of the algorithm, when the first successful measurement on the probe qubit is achieved, the probability of the system being in state $|\Psi_1\rangle$ is $\left|c_1^{(1)}(t_0)\right|^2$ and $c_1^{(1)}(t_0) = c_1'$, while the probability of the system being in state $|\Psi_2\rangle$ is $\varepsilon_0 = \left|c_2^{(1)}(t_0)\right|^2$ and $c_2^{(1)}(t_0) = c_2'$. Then in the purification procedure, the input state of the algorithm is $|\Psi_0^{(1)}\rangle = |1\rangle|0\rangle \left(c_1^{(1)}(t_0)|\varphi_k^{\text{sol}}\rangle + c_2^{(1)}(t_0)|\varphi_k^{\text{non-sol}}\rangle\right)$.

In basis of $\{|\Psi_0^{(1)}\rangle, |\Psi_1\rangle, |\Psi_2\rangle\}$, the Hamiltonian of the algorithm is in the form

$$H = \begin{pmatrix} -\frac{1}{2} & cc_1^{(1)}(t_0) & cc_2^{(1)}(t_0) \\ cc_1^{(1)}(t_0)^* & -\frac{1}{2} & 0 \\ cc_2^{(1)}(t_0)^* & 0 & \frac{1}{2} \end{pmatrix}. \quad (8)$$

This purification procedure can be iterated for a number of times until M successful measurements on the probe qubit are obtained. With the same initial state and evolution time t_0, as the parameter $c_1^{(1)}(t_0)$ becomes larger, the probability of the system being evolved to state $|\Psi_1\rangle$ is larger [16]. Therefore we have the following relation: $\left|c_1^{(1)}(t_0)\right| < \left|c_1^{(2)}(t_0)\right| < \cdots < \left|c_1^{(M)}(t_0)\right| < 1$, and $\left|c_2^{(1)}(t_0)\right| > \left|c_2^{(2)}(t_0)\right| > \cdots > \left|c_2^{(M)}(t_0)\right| > 0$, the converge speed to the state $|\Psi_1\rangle$ of the system is accelerated in the purification process. The first iteration provides the lowest transformation speed to state $|\Psi_1\rangle$. From Fig. 2 and Fig. 3, we can see that $(1-\varepsilon_0) \approx 1 \gg \varepsilon_0$, where $\varepsilon_0 = \left|c_2^{(1)}(t_0)\right|^2$. Based on this, we can conclude that after M successful measurements on the probe qubit, the upper bound for the error (the probability of the system being in state $|\Psi_2\rangle$) in a round of the algorithm is ε_0^M. The probability for the system being in state $|\Psi_1\rangle$ is $1-\varepsilon_0^M$. And unlike the approach in Ref. [17], we do not require M continuous successful measurements of the probe qubit in the purification process of this algorithm. The state that is to be purified is updated in each iteration of the purification procedure. Therefore M successful measurements on the probe qubit can be achieved in polynomial number of trials.

We make a numerical estimation on the success probability of the algorithm. From Fig. 2 and Fig. 3, we can see that $\left|c_1^{(1)}(t_0)\right|^2 : \left|c_2^{(1)}(t_0)\right|^2 > 9:1$, then $\varepsilon_0 < 0.1$. After M successful measurements on the probe qubit, the error in each round of the algorithm can be controlled to be smaller than 0.1^M. The success probability of the algorithm $P_{\text{succ}} = (1-\varepsilon_0^M)^M > \left[1-(0.1)^M\right]^M$. Fig. 4 shows the variation of the success probability of the algorithm P_{succ} vs. M. From the figure we can see that the success probability of the algorithm converges quickly to one even after a few purification iterations.

In practice, the state in each round of the algorithm can be purified in a few iterations such that the state is very close to the solution state of the round of the algorithm, as in the example above, by setting $c = 0.02$, and $t_0 = \pi/2c$, the errors are $\{3.85\times10^{-4}, 1.54\times10^{-7}, 6.18\times10^{-11}\}$, for $M = 1, 2, 3$, respectively. From the expression $P_{\text{succ}} = (1-\varepsilon_0^M)^M$, we can see that the algorithm can still have a high success probability as long as the error is compressed to a certain degree in each round of the algorithm, since the error decreased exponentially with the number of successful measurements. For example, the success probability of the algorithm can be $P_{\text{succ}} = 1/2$, if the error in each round of the algorithm is controlled smaller than $1-2^{-1/M}$. In real implementation of the algorithm, a polynomial large success probability of the algorithm can be achieved by performing only a few iterations of the purification procedure in each round of the algorithm, e.g., by performing only one successful measurement on the probe qubit, the error can be controlled to a degree that guarantees the success probability of the algorithm $P_{\text{succ}} > 1/2$ for $M = 1000$ clauses.

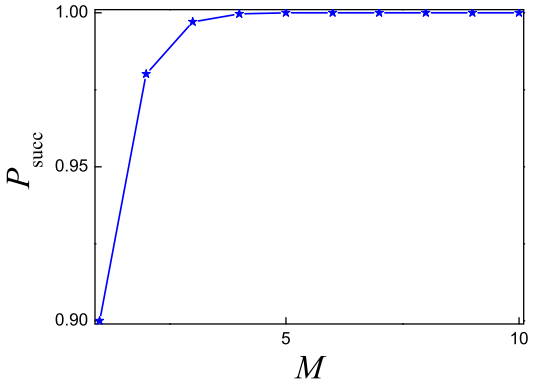

FIG. 4. The success probability of the algorithm vs. the number of successful measurements on the probe qubit, while setting $\varepsilon_0 = 0.1$.

V. DISCUSSION

For an n-bit EC3 problem, classically the probability p for obtaining a solution to the problem is $p = N_M/2^n$, where N_M is the number of the assignments that satisfy all of the M clauses according to the algorithm. In the algorithm, the probability p is decomposed into M steps $p = p_1 p_2 \cdots p_M$, and each p_k is finite. By applying the M clauses sequentially, and using a non-unitary operator through introducing partial measurement, the state that satisfies all of the clauses is projected out step by step. The dimension of the search space of the problem is reduced exponentially in each round of the algorithm. This makes the run time of the algorithm scales linearly with the number of clauses, thus scales polynomial with the number of bits of the problem.

In each round of the algorithm, a state that satisfies the current clause and all of the clauses in previous rounds of the algorithm can be obtained with finite success prob-

ability. We introduce a purification procedure which is based on resonance and partial measurement to purify the solution state of each round of the algorithm, the error in each round of the algorithm decreases exponentially with the number successful measurements on the probe qubit. Therefore the success probability of the algorithm can be polynomial large by compressing the error through the purification procedure, which can be can be achieved in finite number of trials.

ACKNOWLEDGMENTS

We thank Dr. Song Liu for helpful discussions. This work was supported by the National Natural Science Foundation of China (Grant No. 11275145).

[1] E. Chastain, A. Livnat, C. Papadimitriou and U. Vazirani, Proc. Natl. Acad. Sci. **111**, 10620 (2014).
[2] P. Shor, *Proc. 35th Ann. Symp. on Found. of Comp. Sci.*, 124–134 (IEEE Comp. Soc. Press, Los Alamitos, CA, 1994).
[3] L. K. Grover, Phys. Rev. Lett. **79**, 325-328 (1997).
[4] A. M. Childs and W. van Dam, Rev. Mod. Phys. **82(1)**, 1-52 (2010).
[5] I. Buluta and F. Nori, Science, **326**, 108 (2009).
[6] S. Lloyd, Science **273**, 1073 (1996).
[7] S. A. Cook, *Millennium Problems* (Clay Mathematics Institute, 2000), http://www.claymath.org/millennium.
[8] C. Seife, Science **309**, 96 (2005).
[9] E. Farhi, J. Goldstone, and S. Gutmann, *e-print*: quant-ph/0007071v1 (2000)
[10] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, D. Preda, Science **292**, 472-475 (2001).
[11] W. van Dam, M. Mosca, and U. Vazirani, in *Proceedings of the 42th IEEE Symposium on Foundations of Computer Science* (*FOCS 2001*) (IEEE Computer Society, Washington, DC, 2001), p. 279-287.
[12] M. Žnidarič, and M. Horvat, Phys. Rev. A **73**, 022329 (2006).
[13] E. Farhi, J. Goldstone, and S. Gutmann, *e-print*: quant-ph/0208135 (2002).
[14] E. Farhi, et al., Int. J. Quantum. Inform. **6**, 503-516 (2008).
[15] I. Hen, A. P. Young, Phys. Rev. E **84**, 061152 (2011).
[16] H. Wang, *e-print* arXiv: 1510.00820v1 (2015).
[17] H. Nakazato, T. Takazawa and K. Yuasa, Phys. Rev. Lett. **90**, 060401 (2003).
[18] H. Wang, Phys. Rev. A **93**, 032301 (2016).
[19] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. (Cambridge Univ. Press, Cambridge, England, 2000).